«Cyberspace does not lie within your borders» – Jurisdiktion und Menschenrechte im digitalen Raum

Langer, Lorenz

Swiss Review of International and European Law

Schweizerische Zeitschrift
für internationales und europäisches Recht

Revue suisse de droit international et européen

Volume 29 (2019), Number 1

Schulthess §

Swiss Review of International and European Law

Schweizerische Zeitschrift für internationales und europäisches Recht

Revue suisse de droit international et européen

ISSN 1019-0406 www.sriel.ch

The Review is published quarterly by the Swiss Society of International Law (Schweizerische Vereinigung für internationales Recht / Société suisse de droit international – www.svir-ssdi.ch) and supported by the Swiss Academy of Humanities and Social Sciences. The Review is available online on www.swisslex.ch and www.heinonline.org.

Submissions
Please submit manuscripts electronically to the Managing Editor (Lorenz.Langer@sriel.ch). Authors are requested to follow the Reivew's style-sheet available at www.sriel.ch. French submissions are proofread by Dr. Maria Ludwiczak Glassey.

Publishers
Schulthess Juristische Medien AG
Zwingliplatz 2, Postfach, CH-8021 Zurich, Internet: www.schulthess.com
Managing Publisher: Firas Kharrat
Product Manager Journals: Christian Hillig

Customer Service
E-Mail: service@schulthess.com
Tel. +41 44 200 29 29
Fax +41 44 200 29 28
Anschrift: Schulthess Juristische Medien AG, Kundenservice, Zwingliplatz 2, Postfach, CH-8021 Zürich

Subscriptions
Annual subscription: CHF 250
Annual preferential subscription: for members of the Swiss Society of International Law CHF 242
Single issue: CHF 74, plus postage
All subscription prices incl. 2.5% VAT, plus postage: CHF 8 in Switzerland (Postage Abroad: CHF 43).
Vorzugspreis gegen Vorlage eines gültigen Nachweises. Subscriptions are automatically extended each year unless notice of cancellation is received from the subscriber prior to 8 weeks in advance of the subscription period.

Advertisements
Zürichsee Werbe AG, Herr Pietro Stuck, Seestrasse 86, CH-8712 Stäfa, Tel. +41 44 928 56 11,
E-Mail: pietro.stuck@zs-werbeag.ch

Frequency
The Review is published quarterly, volume 29

Citation
29 SRIEL (2019) p. 1

Internet
www.sriel.ch
The Review is also available online at www.heinonline.org

ISSN 1019-0406

Table of Contents

«Cyberspace does not lie within your borders» – Jurisdiktion und Menschenrechte im digitalen Raum

Lorenz Langer*

Inhalt

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. ...*
> *Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. ...*
>
> John P. Barlow, A Declaration of the Independence of Cyberspace[1]

1. Menschenrechte und Territorialität

Vor etwa drei Jahren fuhr ein weisser Jeep Cherokee auf der Interstate 64, der Autobahn im Westen von St. Louis, Missouri. Auf einer Überführung ohne Pannenstreifen verlangsamte der Jeep plötzlich; die folgenden Fahrzeuge mussten abrupt abbremsen, ein grosser Lastwagen konnte nur knapp ausweichen. Dieses gefährliche Manöver war nicht die Schuld des Fahrers – sondern zweier Hacker, die von einem

* Managing Editor; Zentrum für Demokratie Aarau, Universität Zürich; Liechtenstein-Institut, Bendern (FL). – Dieser Kommentar beruht auf einem im Oktober 2018 an der Universität Wien gehaltenen Referat; der Vortragsstil wurde weitgehend beibehalten. Ich danke Sara Pangrazzi, Andreas Th. Müller und Teresa Kam herzlich für ihre Unterstützung und Kommentare.

1 John Perry Barlow, A Declaration of the Independence of Cyberspace 8. Februar 1996, <https://www.eff.org/de/cyberspace-independence>, al. 1, 3.

Sofa aus mittels Mobilfunknetzwerk die Kontrolle über das Fahrzeug übernommen und auf Leerlauf geschaltet hatten.[2]

Zum Glück handelte es sich dabei um ein Versuchssetting – auch wenn der Journalist am Steuer nicht genau gewusst hatte, was ihn erwartete, und über die Possen der Programmierer auch wenig erbaut war. Unter anderen Vorzeichen hätte diese Situation viel schlimmer ausgehen können: Ein schwerer Unfall auf der Autobahn wäre durch einen solchen Cyber-Angriff schnell verursacht.

Nun soll man von seinen Nächsten nichts Böses denken – weder von Individuen noch von Staaten. Aber die Ereignisse neuester Zeit legen nahe, dass manche staatlichen Akteure vor kaum etwas zurückschrecken, wenn sie etwa gegen ihnen unliebsame Personen im Ausland vorgehen wollen.[3] Eine solche Verletzung des völkerrechtlichen Interventionsverbotes mag für die Urheber diplomatische, wirtschaftliche, vielleicht sogar militärische Konsequenzen haben. Es stellt sich aber auch die Frage, ob diese Staaten zugleich gegen *menschenrechtliche* Verpflichtungen verstossen, die sie eingegangen sind.

Die extraterritoriale Anwendung von Menschenrechtsverträgen wirft komplexe Probleme auf.[4] Die Lösung dieser Probleme ist aber besonders anspruchsvoll, wenn es sich bei einer solchen Aktion um einen sogenannten «Cyberangriff» handelt – also um eine Instrumentalisierung von Informationstechnologie, die voraussichtlich Menschen verletzt oder tötet bzw. Sachschäden verursacht.[5] Das Beispiel des Jeep Cherokee zeigt, dass der Zugriff auf ein Individuum sehr viel einfacher ist, wenn er auf elektronischem Wege stattfindet, anstatt dass zwei oder gar fünfzehn «Touristen» in das jeweilige Land entsendet oder zwei angebliche Lockvögel für «Versteckte Kamera» angeworben werden müssen.[6]

2 Andy Greenberg, «Hackers Remotely Kill a Jeep on the Highway–With Me in It», Wired, 21. Juli 2015, <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

3 So zuletzt die Giftanschläge auf Kim Jong Nam im Februar 2017 (Anna Fifield, «Kim Jong Un's Half Brother Killed in Apparent Poison Attack», Washington Post, 15. Februar 2017, S. A10) und auf Sergei Skripal in Salisbury im März 2018 (Vikram Dodd & Andrew Roth, «Salisbury Novichok Suspects Say They Were Only Visiting Cathedral», Guardian, 13. September 2018), sowie die Ermordung von Jamal Ahmad Khashoggi in Istanbul im Oktober 2018 (Inga Rogg, «Türkische Ermittler legen nach», Neue Zürcher Zeitung, 13. Oktober 2018, S. 3).

4 Allgemein Marko Milanovic, Extraterritorial Application of Human Rights Treaties, Oxford 2011.

5 Vgl. Michael N. Schmitt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, New York 2013, S. 15 sowie Rule 30. Zur Problematik der Begrifflichkeit Oliver Diggelmann & Nina Hadorn, «Gewalt- und Interventionsverbot bei Cyberangriffen», in: Christian Schubel et al. (Hg.), Jahrbuch für Vergleichende Staats- und Rechtswissenschaften 2016/2017, Baden-Baden 2017, S. 260–261.

6 Vgl. Lizzie Dearden, «Novichok Suspects Insist They Were 'Sightseeing'», Independent, 14. September 2018, S. 6; Rogg, supra, Fn. 3, S 3; Nile Bowie, «Woman Accused of Killing Kim Jong Un's Half-brother Walks Free», Asia Times, 11. März 2019, <https://www.asiatimes.com/2019/03/article/woman-accused-of-killing-kim-jong-uns-half-brothers-walks-free/>.

Können Staaten auch für etwaige Menschenrechtsverletzungen im oder via Cyberspace zur Verantwortung gezogen werden? Die meisten Menschen dürften auf diese Frage mit «ja, natürlich» antworten. Denn Menschenrechte stehen, wie der Begriff impliziert, dem Individuum *qua* Mensch zu: als Attribut des Menschseins. Dies machte schon – zumindest in der Theorie – die *Virginia Declaration of Rights* von 1776 deutlich: Grundreche sind inhärent und können weder aberkannt noch aufgegeben werden.[7] Die inzwischen klassische Formulierung dieses Grundsatzes wurde 1993 in Wien anlässlich der Weltmenschenrechtskonferenz adoptiert. Danach sind Menschenrechte universell und unteilbar, sie bedingen sich gegenseitig und stehen folglich in einer Wechselbeziehung.[8]

Die ersten Menschenrechtserklärungen der Neuzeit implizierten aber zugleich auch, dass die postulierten Rechte nicht unterschiedslos gewährt und garantiert werden. Der Grund- oder Menschenrechtsschutz war vielmehr persönlich und räumlich eingeschränkt. Die *persönliche* Beschränkung wird etwa bei der *Déclaration des droits de l'homme et du citoyen* von 1789 deutlich, die *tous les membres du corps social* schützt – also nur die Mitglieder des jeweiligen (hier französischen) Gemeinwesens.[9] Die *territoriale* Beschränkung hingegen ist beispielsweise besonders deutlich formuliert im Ingress des österreichischen Staatsgrundgesetzes von 1867, das zwar bereits einen vergleichsweise fortschrittlichen Katalog durchsetzbarer Grundrechte enthielt, dessen Geltung jedoch explizit auf das Gebiet Cisleithaniens beschränkte.[10]

Dieses primär *territoriale* Verständnis von Grund- und Menschenrechtsschutz prägte auch die Entstehungsgeschichte der modernen regionalen oder internationalen Menschenrechtsinstrumente. Gemäss Art. 1 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten sichern die Signatarstaaten die

7 Virginia Declaration of Human Rights vom 12. Juni 1776, Art. I: *«That all men are by nature equally free and independent, and have certain inherent rights, of which, when they enter into a state of society, they cannot, by any compact, deprive or divest their posterity; …»* (abgedruckt in Bardo Fassbender (Hg.), Quellen zur Geschichte der Menschenrechte: Von der Amerikanischen Revolution zu den Vereinten Nationen, Universal-Bibliothek, Stuttgart 2014, S. 6).

8 Vienna Declaration and Programme of Action, World Conference on Human Rights, 25. Juni 1993, U.N. Doc. A/CONF.157/24 (Part I), Para. 5: *«All human rights are universal, indivisible and interdependent and interrelated»*.

9 Déclaration des droits de l'Homme et du citoyen vom 26. August 1789, Préamble (abgedruckt in Fassbender, supra, Fn. 7, S. 42). Innerhalb des *corps social* waren wiederum primär die Männer Rechtsträger, vgl. dagegen schon Olympe de Gouges, Déclaration des droits de la femme et de la citoyenne, Paris 1791. – Noch umfassender war der Ausschluss der afro-amerikanischen Bevölkerung in den USA, der weder in der Unabhängigkeitserklärung noch in der Verfassung explizit gemacht wurde.

10 Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, 21. Dezember 1867, StF: RGBl 1867/142 (Kaiserreich Österreich), Ingress. Allgemein Gabriele Kucsko-Stadlmayer, «Die allgemeinen Strukturen der Grundrechte», in Detlef Merten et al. (Hg.), Grundrechte in Österreich, 2. Aufl., Heidelberg 2014, 77–137, Rz. 4.

Konventionsrechte allen Personen innerhalb ihrer «Jurisdiktion» zu;[11] mit dem Begriff der «Hoheitsgewalt» betont die deutsche Übersetzung das Element der tatsächlichen Kontrolle zusätzlich.[12] Die *travaux préparatoires* zur Konvention belegen, dass diese Formulierung und das Konzept der Jurisdiktion eindeutig territorial verstanden wurden.[13] Auch beim Uno-Pakt über die bürgerlichen und zivilen Rechte zeigt die historische Auslegung des einschlägigen Artikels 2, dass Staaten grundsätzlich nicht für Individuen verantwortlich sein wollten, die sich ausserhalb ihres Hoheitsgebietes aufhalten – selbst wenn diese etwa aufgrund des Personalitätsprinzips ihrer Gerichtsbarkeit unterstünden.[14]

2. Die Relativierung territorialer Kriterien

Die Garantie von Menschenrechten – und die Verantwortlichkeit für deren Verletzung – ist im Ursprung also grundsätzlich an ein Terrain gebunden. Dieses territoriale Element war aber traditionellerweise nicht nur ein Charakteristikum des Menschenrechtsschutzes, sondern auch des Völkerrechts allgemein: Als *inter*nationales Recht, als *ius inter nationes,* sind ihm Grenzen und damit Territorien begriffsnotwendig.[15]

Gerade im Zusammenhang mit der Globalisierung wird nun aber im Völkerrecht ein Prozess der zunehmenden «Entterritorialisierung» postuliert.[16] Am offensichtlichsten ist dieser Prozess bei wirtschaftlichen Fragen. So wurde ein Welthandelssystem errichtet, das nationale bzw. territoriale Handelshemmnisse zu minimieren sucht; auch internationale Finanzströme fliessen heute häufig ungehemmt, ja unkon-

11 European Convention for the Protection of Human Rights and Fundamental Freedoms, 4. November 1950, C.E.T.S. 5, Art. 1: *«to everyone within their jurisdiction»,* bzw. *«à toute personne relevant de leur juridiction»*.

12 In der offiziellen deutschen Übersetzung (BGBl. II S. 1198; SR 0.101): «Die Hohen Vertragsparteien sichern allen ihrer Hoheitsgewalt unterstehenden Personen die in Abschnitt I bestimmten Rechte und Freiheiten zu». Die österreichische und liechtensteinischen Übersetzungen verwendet statt «Hoheitsgewalt» den Begriff «Jurisdiktion» (BGBl. Nr. 210/1958 (Stammfassung); LGBl-Nr. 1982.060.001). Dieser Terminus fand sich ursprünglich auch in der deutschen Fassung der Schweiz (AS 1974 2151; der Wechsel erfolgte mutmasslich mit dem 11. Zusatzprotokoll, vgl. SR 0.101, Stand vom 28. Mai 2002).

13 Council of Europe, Collected Edition of the ‹Travaux Préparatoires› of the European Convention on Human Rights Den Haag 1975–85, Bd. III, S. 260. Vgl. dazu *Banković and others v. Belgium and others,* Application no. 52207/99, ECtHR (Grand Chamber), 12. Dezember 2001, Para. 19–21.

14 In diesen Fällen müsste ggf. diplomatischer Schutz angerufen werden: Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary, 2. Aufl., Kehl 2005, Art. 2 Rz. 27.

15 Dies gilt zumindest für das Bedeutungsfeld des Begriffs der Nation seit dem Spätmittelalter, vgl. Reinhart Koselleck, «Volk, Nation, Nationalismus, Masse», in: O. Brunner et al. (Hg.), Geschichtliche Grundbegriffe, Bd. 7, Stuttgart 1992, 143, 282–284.

16 Vgl. beispielsweise Daniel Bethlehem, «The End of Geography: The Changing Nature of the International System and the Challenge to International Law», 25 European Journal of International Law (2014), S. 9. Kritisch Lorenz Langer «The South China Sea as a Challenge to International Law and to International Legal Scholarship», 36 Berkeley Journal of International Law (2018), S. 384–386.

trollierbar. Neben wirtschaftlichen Aspekten liegen aber auch sogenannte *global commons* – etwa die Umwelt, aber auch der Schutz der Gesundheit – zunehmend ausserhalb der Regelungsfähigkeit einzelner Staaten.

Beim Menschenrechtsschutz spielen Ereignisse jenseit der eigenen Staatsgrenzen ebenfalls eine zunehmende Rolle und relativieren den territorialen Fokus zumindest graduell. So ist etwa beim Gebot des *non-refoulement* nicht die Menschenrechtslage im eigenen Land relevant: Die Rückschaffung in ein Drittland ist dann verboten, wenn *dort* Folter oder unmenschliche Behandlung droht.[17] Militärisches Engagement im Ausland kann inzwischen auch menschenrechtliche Verantwortung zur Folge haben.[18] Menschenrechtsverstösse wie Menschenhandel weisen fast immer transnationale Aspekte auf,[19] und als zunehmend inadäquat wird schliesslich auch die rein nationalrechtliche Reaktion auf internationale Flüchtlings- und Migrationsströme erkannt; deren menschenrechtliche Implikationen werden deshalb immer häufiger vor internationalen Gerichten verhandelt.[20]

3. Der Cyberspace

Wir beobachten hier also eine Entwicklung weg vom traditionellen territorialen Rechtsverständnis. Und dieselbe Problematik der «Enträumlichung» stellt sich noch viel dringlicher und akuter im Zusammenhang mit der Digitalisierung. Das Phänomen der Digitalisierung und des Cyberspace beschäftigt inzwischen natürlich auch das Recht und die Rechtswissenschaft. Neue Gesetze und Konventionen treten in Kraft, um – wie es die Budapester Konvention formuliert – den «tiefgreifenden Veränderungen» gerecht zu werden, welche «die Digitalisierung, Konvergenz und fortdauernde Globalisierung von Computernetzwerken» mit sich bringen.[21] Hier

17 Vgl. *Soering v. United Kingdom,* Application no. 14038/88, ECtHR (Plenary), 7. Januar 1989; unvereinbar damit bleibt also etwa die Rückschaffung von Terroristen in Folterstaaten, auch wenn diese politisch opportun wäre (vgl. Motion Fabio Regazzi, Ausweisung von Terroristinnen und Terroristen in ihre Herkunftsländer, unabhängig davon, ob sie als sicher gelten oder nicht, Nationalrat, Curia Vista 16.3982, 13. Dezember 2016 (von beiden Räten angenommen)).

18 Vgl. *Al-Jedda v. United Kingdom,* Application no. 27021/08, ECtHR (Grand Chamber), 7. Juli 2011, und *Al-Skeini and Others v. United Kingdom,* Application no. 55721/07, ECtHR (Grand Chamber), 7. Juli 2011.

19 Vgl. *J. and Others v. Austria,* Application no. 58216/12, ECtHR (Chamber), 17. Januar 2017.

20 *E.g. Hirsi Jamaa and Others v. Italy,* Application no. 27765/09, ECtHR (Grand Chamber), 23. Februar 2012; *N.D. & N.T. v. Spain,* Application nos. 8675/15 & 8697/15, ECtHR (Chamber), 3. Oktober 2017, (Anhörung vor der Grossen Kammer am 26. September 2018).

21 Convention on Cybercrime [Budapest Convention], 23. November 2001, E.T.S. 185, Preamble, al. 4: *«Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; …»*. S. dazu auch die Beiträge des 43. Österreichischen Völkerrechtstags, Welches (Völker)Recht gilt im Cyberspace? Ludwig-Maximilians-Universität München, 18.–20. Mai 2017 (publiziert in: 73 Zeitschrift für Öffentliches Recht (2018), S. 3–135).

stehen wir potentiell nicht nur vor einer graduellen Veränderung, sondern vor einem eigentlichen Paradigmenwechsel. Denn das traditionelle Verständnis und auch die traditionelle Terminologie, um physischen Raum zu regulieren, ja überhaupt zu beschreiben, sind hier nur noch beschränkt adäquat.

Aber was genau bezeichnet der allgegenwärtige Begriff des *Cyberspace* eigentlich? Es gibt kein deutsches Synonym für diesen Portemanteau aus *cybernetic* und *space*.[22] Der Begriff geht zurück auf eine Kurzgeschichte von William Gibson und bezeichnet dort die «konsensuale Massenhalluzination» *(mass consensual hallucination)* in Computernetzwerken.[23] An anderer Stelle beschreibt er den Cyberspace als *«lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.»* [24] Andere Definitionen sind etwas nüchterner, wenn auch kaum greifbarer;[25] sie unterstreichen aber ebenfalls den körperlosen Charakter dieses «Raums». Offenbar bereitet es Mühe, diese Entität zu umschreiben, und erst recht, sie sich bildhaft vorzustellen. Es ist bemerkenswert, wie (im typographischen Sinn) stereotyp unsere einschlägigen Vorstellungen geblieben sind. Beispielhaft dafür ist die frühe Darstellung einer «Datenwelt» im Film *Tron,* die sich auch in der Fortsetzung knapp 30 Jahre später kaum verändert hat.[26]

Wie schwer wir uns mit der Vorstellung einer virtuellen elektronischen Sphäre tun, zeigt auch die Terminologie, die weitgehend auf Analogien angewiesen ist. Zuerst ist der *Cyberspace* ja eigentlich ein Nicht-Raum. Auch gibt es im Cyberspace keine Grenzen im herkömmlichen Sinn, und trotzdem sprechen wir von «Brandmauern» bzw. *Firewalls*. Offensichtlich sind hier traditionelle Konzepte selbst bei analogischer Verwendung von beschränktem Nutzen, ja vielleicht sogar irreführend. Denn es handelt sich um essentielle, nicht graduelle Unterschiede: Am ehesten könnte man den Schritt von der Alltagswelt in den Cyberspace vielleicht mit dem Sprung von der klassischen Physik zur Quantenmechanik vergleichen.

22 Zur Etymologie s. «cyberspace, n.», in Oxford English Dictionary, 3. Aufl. 2010: «Etymology: < ancient Greek κυβερνήτης steersman (see cybernetics n.) + -ic suffix. Compare ancient Greek κυβερνητικός good at steering».

23 William Gibson, «Burning Chrome», 4 Omni (1982), 72–77.

24 William Gibson, Neuromancer, New York 1984, 69. – Gibson selbst bezeichnete den Begriff später als grundsätzlich sinnentleertes, aber evokatives und effektives Schlagwort: *«All I knew about the word <cyberspace> when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless»* (William Gibson – No Maps for These Territories (Regie: Mark Neale), Grossbritannien 2000, bei Min. 54).

25 *E.g.* Michael Benedikt, Cyberspace: First Steps, Cambridge, Mass. 1992, S. 122: *«Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial, or <virtual> reality. In this reality, to which every computer is a window, seen or heard objects are neither physical nor, necessarily, representations of physical objects but are, rather, in form, character and action, made up of data, of pure information.»*

26 Tron (Regie: Steven Lisberger, USA 1982); Tron Legacy (Regie: Joseph Kosinski, USA 2010). – In der dystopischen «Matrix»-Franchise (Regie: Lana & Lilly Wachowski, USA 1999–2005) wiederum ist gerade die «reale» Welt virtueller Natur.

Diese Unbestimmtheit beschlägt auch unsere gewohnte Vorstellung von Normsetzung und -durchsetzung. Zu Beginn wurde der Cyberspace als – je nach Perspektive – gesetzloser oder freier Raum projiziert, verbunden mit der Befürchtung bzw. der Hoffnung, dass dieser Raum dem Zugriff der Staaten entzogen bliebe. Die letztere, idealistische Sichtweise veranschaulicht etwa die bereits eingangs zitierte «Unabhängigkeitserklärung des Cyberspace», welche John Perry Barlow 1996 am *World Economic Form* veröffentlichte:[27] Der Cyberspace liege ausserhalb jeglicher staatlicher Souveränität; die Regierungen, diese «erschöpften Giganten aus Fleisch und Stahl», hätten deshalb keinerlei Recht, die digitale Sphäre zu regulieren. Die hergebrachten gesetzlichen Konzepte seien im immateriellen Cyberspace obsolet; dessen körperlose Bewohner blieben der staatlichen Zwangsgewalt entzogen. Unter einem neuen Gesellschaftsvertrag würden diese Bewohner vielmehr ein selbst-regulierendes und freiheitliches Utopia schaffen:

> We have no elected government, nor are we likely to have one … . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[28]

> You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.[29]

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.[30]

> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

> Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[31]

27 Barlow, supra, Fn. 1.
28 Barlow, supra, Fn. 1, al. 2.
29 Barlow, supra, Fn. 1, al. 4.
30 Barlow, supra, Fn. 1, al. 6.
31 Barlow, supra, Fn. 1, al. 8–10.

We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.[32]

Diese Erklärung atmete nicht nur den Geist der unabhängigen und wegweisenden *academic hackers* der 1960er- und 1970er-Jahre,[33] sondern auch der Gegenkultur jener Ära.[34] Heute wirkt ihr Idealismus nicht nur etwas anachronistisch, sondern auch weltfremd. Das Internet ist heute mitnichten eine herrschaftsfreie Sphäre, die sich staatlichen Sanktionen entzieht.[35] Und ebenso ist es inzwischen offensichtlich, dass rechtliche Konzepte sehr wohl relevant sind im Cyberspace – für praktisch *alle* Rechtsgebiete, vom Strafrecht bis zum Medienrecht. Zwar wurde anfänglich noch argumentiert, dass es sich beim Cyberspace um *global commons* handle, analog etwa zur Hochsee oder zum Weltraum.[36] Die Konzeptualisierung der Normierung erfolgte dann aber primär territorial, selbst für Verbrechen *im* Internet.[37]

Wie schwer die Lösung von traditionellen Vorstellungen auch im Völkerrecht ist, verdeutlicht das sogenannte Tallinn Manual, das inzwischen in der «Version 2.0» erschienen ist.[38] Es handelt sich um einen von einer Expertengruppe und unter Schirmherrschaft der NATO verfassten Kodifizierungsvorschlag für Cyberangriffe. Auch hier wird hartnäckig versucht, mit traditionellen völkerrechtlichen Konzepten – Souveränität, Staaten-Immunität etc. – staatliches Handeln im Cyberspace zu erfassen. Das ist zumindest insofern nachvollziehbar, als dass der Cyberspace an physische Infrastrukturen wie Server und Leitungen oder Kabel gebunden bleibt. Gemäss Tallinn-Manual behält das Konzept der Souveränität für diese Infrastruktur seine Relevanz, ebenso wie für die Verbindungen zwischen solchen physischen Komponenten und für die Personen, welche im Cyberspace aktiv werden.[39] Daraus folgt zugleich, dass die Aktivitäten eines Staates im Cyberspace durch die spiegelbildliche

32 Barlow, supra, Fn. 1, al. 15.

33 Vgl. Eric S. Raymond, The Art of Unix Programming, Boston 2004, S. 44.

34 J.P. Barlow (1947–2018) war nicht nur Mitbegründer der *Electronic Frontier Foundation,* einer Nichtregierungsorganisation, sondern (u.a.) auch Songtexter der Rockband *Grateful Dead*: Sam Roberts, «John Perry Barlow, 70, Champion of an Open Internet, Dies», New York Times, 9. Februar 2018, S. B14.

35 Die «*methods of enforcement*» werden vielmehr immer effektiver, s. Freedom House, Freedom on the Net 2018, 12. Oktober 2018, <https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf>.

36 Yaroslav Radziwill, Cyber-attacks and the Exploitable Imperfections of International Law, Leiden 2015, S. 92.

37 Art. 22 Budapest Convention (Jurisdiction): [1] Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction [...] when the offence is committed: a) in its territory; or b) on board a ship flying the flag of that Party; b on board a ship flying the flag of that Party; or c) on board an aircraft registered under the laws of that Party; [...].

38 Michael N. Schmitt (Hg.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, 2. rev. Aufl., Cambridge 2017.

39 Schmitt, supra, Fn. 38, Rule 1(4), S. 12.

Souveränität anderer Staaten begrenzt wird. Hier stellen sich zahlreiche und komplizierte Fragen in Zusammenhang mit dem Interventionsverbot, dem Gewaltverbot und ggf. dem Recht auf Selbstverteidigung.

4. Cyberspace und Menschenrechte

Die besondere Beschaffenheit des Cyberspace hat aber auch Implikationen für die Menschenrechte. Die Digitalisierung ist eine Herausforderung für deren rechtlichen Schutz, und zwar in doppelter Hinsicht: Zuerst werden Grund- und Menschenrechte zunehmend gefährdet durch das Handeln Dritter im Internet, etwa durch illegale Pornographie oder Datendiebstahl, vor allem aber auch durch *hate speech* oder *cybermobbing*. Die staatliche Definition und Sanktionierung digitaler Tatbestände und damit die Überwachung des Internets nimmt als Folge stetig zu. Auf internationaler Ebene sind digitale Formen der Kinderpornographie bereits Gegenstand der Budapester Konvention;[40] das Zusatzprotokoll zur Budapester Konvention verpflichtet die Signatarstaaten auch, die Verbreitung rassistischer und xenophober Inhalte durch Computersysteme zu kriminalisieren.[41] Eine solche Vorschrift wäre in einer *universell* anwendbaren Konvention aber bereits schwer vorstellbar, kollidierte sie doch mit dem extensiveren sachlichen Schutzbereich der Meinungsäusserungsfreiheit, wie er etwa in den Vereinigten Staaten gilt.[42]

Im Schnittbereich von Internet und Menschenrechtsschutz stand denn auch lange nicht die Erwartung im Vordergrund, dass Regierungen Menschenrechte auf dem Internet schützten, sondern vielmehr die Furcht vor staatlichen Einschränkungen der Freiheitsrechte im Cyberspace. Dies galt und gilt vor allem in Bezug auf den Zugang zum Internet: Stichworte sind hier *Open Internet* und *Digital Rights*.[43] Relevant ist in diesem Zusammenhang primär die Meinungsäusserungs- und Informationsfreiheit bzw. deren Gefährdung durch Zensur, durch Firewalls oder durch die Beschränkung der *net neutrality*.[44] Ein effektiver Menschenrechtsschutz verlangt hier vor allem staatliche Untätigkeit: also den Schutz des *status negativus* gemäss

40 Art. 9 Budapest Convention. Hier steht der Inhalt im Vordergrund, während sich das übrige materielle Strafrecht der Konvention (Chapter II, Section 1: Substantive Criminal Law) primär am *Medium* einer Rechtsverletzung orientiert.

41 Art. 3 Abs. 1 Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, 28. Januar 2003, E.T.S. 189.

42 S. dazu Lorenz Langer, Religious Offence and Human Rights, Cambridge 2014, 280–290.

43 Vgl. Wolfgang Benedek, «Internet Governance and Human Rights», in: Wolfgang Benedek et al. (Hg.), Internet Governance and the Information Society, Utrecht 2008, S. 31–50.

44 Die entsprechenden Befürchtung fanden auch in der Budapest-Konvention – zumindest in der Präambel – ihren Niederschlag (al. 8 und 9).

Georg Jellinek oder, in politischer Hinsicht, der *negative liberty* Isaiah Berlins:[45] Die Individuen sollen die kommunikativen und kommerziellen Möglichkeiten des Internets möglichst ohne staatliche Einschränkung nutzen können[46] – was in Zeiten eines gesteigerten Sicherheitsbedürfnisses und einer diffuser Bedrohungslage keineswegs selbstverständlich ist.[47]

Positive Obligationen der Staaten sind unstrittig, wenn sie bereits anerkannte Gewährleistungspflichten – etwa zum Schutz der Medienfreiheit oder des Privatlebens – in den digitalen Raum ausweiten.[48] Inwieweit solche Obligationen auch bezüglich Zugang zum Internet und dessen Nutzung bestehen, ist weniger klar.[49] Aber ob nun der *status negativus* oder *positivus* im Vordergrund steht: In Bezug auf den *Geltungsbereich* von Menschenrechtsgarantien wurde im Cyberspace keine grundlegend neue Situation erkannt. Regierungen werden zwar in der elektronischen Dimension aktiv; wenn sie dabei Individualrechte verletzen, so die implizite Annahme, dann befinden sich die Opfer in der Regel innerhalb des staatlichen Territoriums.

45 Georg Jellinek, System der subjektiven öffentlichen Rechte 2., Aufl., Tübingen 1905, S. 87; Isaiah Berlin, «Two Concepts of Liberty», in: Ders., Liberty: Incorporating ‹Four Essays on Liberty›, Oxford 2002, S. 168 (Erstpublikation 1958).

46 *E.g. Ahmet Yıldırım v. Turkey,* Application no. 3111/10, ECtHR (Chamber), 18. Dezember 2012, Para. 10.

47 Von staatlicher Seite werden primär Sicherheitsbedenken als Rechtfertigung für die (versuchte) Regulierung des Internets angeführt; dieses Narrativ eines unausweichlichen *trade-off,* eines Nullsummenspiels zwischen Sicherheit oder Freiheit und Privatsphäre (vgl. Lawrence Wright, «The Spymaster», New Yorker, 21 January 2008, S. 52) hat sich weitgehend durchgesetzt und zu einer markanten Verschiebung der Prioritäten geführt: Zunehmend gilt der Grundsatz *in dubio pro securitate.* Dies ist besonders offensichtlich in den Vereinigten Staaten, wo die Enthüllungen von Edward Snowden zur elektronischen Spionage nur vorübergehend zu einer höheren Gewichtung der Privatsphäre führten (Pew Research Center, The State of Privacy in post-Snowden America, 21. September, Washington D.C. 2016, <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>). In Europa mag sich dieser Wandel verzögern (Christian Reuter, Gordian Geilen & Robin Gellert, «Sicherheit vs. Privatsphäre», in: Heinrich C. Mayr & Martin Pinziger (Hg.), INFORMATIK 2016, Bonn 2016, s. 1759–1773). Aber die Regierungen priorisieren (auch aus politischen Gründen) in der Regel die Sicherheit (vgl. etwa das österreichische «Sicherheitspaket», das im Mai 2018 in Kraft trat und vom Bundesinnenminister als «Firewall für die Bevölkerung» bezeichnet wurde: Bundesministerium Inneres, «Sicherheitspaket ist wie eine Firewall für die Bevölkerung»: Artikel Nr. 15618, 23. Februar 2018, <https://www.bmi.gv.at/news.aspx?id=6B3470332B3046763850773D>). Und die klare Zustimmung des Schweizer Stimmvolks zum revidierten Nachrichtendienstgesetz hat deutlich gemacht, dass auch die Bevölkerung das Sicherheitsargumente ggf. höher gewichtet als rechtsstaatliche Argumente: Peter Siegenthaler, «Entscheid für mehr Sicherheit und weniger Privatsphäre», Swissinfo, 25. September 2016, <https://www.swissinfo.ch/ger/wirtschaft/nachrichtendienstgesetz-ndg-_entscheid-fuer-mehr-sicherheit-und-weniger-freiheit/42469402>.

48 *E.g. Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* Application no. 33014/05, (Chamber), 5. Mai 2011, Para. 64; *K.U. v. Finland,* Application no. 2872/02, ECtHR (Chamber), 2. Dezember 2008, Para. 49 (immerhin mit der in diesem Kontext nicht unbedeutenden Einschränkung, wonach *«a positive obligation … does not impose an impossible or disproportionate burden on the authorities»,* para. 48).

49 S. *e.g.* Paul De Hert & Dariusz Kloza, «Internet (Access) as a New Fundamental Right», 3 European Journal of Law & Technology (2012), <http://ejlt.org/article/view/123/268>.

Der Cyberspace erlaubt es aber dem Staat oder ihm zuzuordnenden Akteuren, gerade auch über die eigenen Grenzen hinaus, ja global zu agieren. Und damit besteht auch das Potential, Menschenrechte weltweit zu verletzen. Die Individuen, deren Rechte kompromittiert werden, müssen sich keineswegs im eigenen Staatsgebiet aufhalten.

Dieses Risiko wird bis jetzt ungenügend thematisiert. Bei sogenannten *cyber-attacks* standen bisher vor allem der Einsatz von Schadsoftware im Vordergrund, oder das Eindringen in Computersysteme. Selbst wenn dies durch staatliche Akteure geschieht, ist der Bezug zu Menschenrechtsgarantien nicht sofort evident: Wenn etwa ein Virus wie *Stuxnet* in die Steuerung von Frequenzumrichtern eingreift und damit Zentrifugen beschädigt, so sind unmittelbar keine Individualrechte betroffen.[50] Das bedeutet aber nicht, dass diese Rechte nicht exponiert wären.

Die Risiken illustriert das eingangs beschriebene, elektronische «Kapern» eines Fahrzeuges. Während ein Auto früher fast ausschliesslich maschinell funktionierte, wird es heute ganz überwiegend elektronisch gesteuert: So gibt es etwa keine mechanische Verbindung zwischen Pedal und Bremse mehr, sondern die Bremsen werden mit einem elektronischen Signal aktiviert.[51] Dazu kommt das sogenannten *internet of things,* also die Verbindung von praktisch jedem elektronischen Gerät mit dem Internet – vom Kühlschrank bis zum Kernkraftwerk, von Flugdrohnen ganz zu schweigen. Aber auch moderne Insulinpumpen und Schrittmacher sind teilweise schon online.[52]

Das Missbrauchspotential ist offensichtlich. Es hat immer etwas leicht obszönes, wenn in den Medien möglichst verheerende Terror-Szenarien imaginiert werden. Wovon man nicht sprechen *sollte,* darüber *kann* man ja durchaus auch schweigen. Aber es braucht nicht allzu viel Phantasie, um sich vorzustellen, welche Menschenrechte hier gefährdet sein könnten. Durch das «Hijacken» eines Fahrzeugs kann ein einzelner Dissident eliminiert werden – erst recht, wenn es sich dabei um ein «autonomes» Vehikel handelt. Ein Cyber-Angriff auf ein Flugzeug oder auf sog. kritische Infrastrukturen wie Spitäler, Staudämme, Kraftwerke und Schienennetze können das Recht auf Leben in grossem, ja ungeheurem Massstab gefährden und verletzen. Ebenso können staatliche Überwachungsmassnahmen das Recht auf Privatheit massiv verletzen.[53]

«Dank» des Cyberspace ist dabei die Ausübung hoheitlicher Gewalt keineswegs auf das eigene Territorium beschränkt. Damit stellt sich die grundlegende Frage, ob diese Art von Handlung angesichts der prinzipiell territorialen Anwendung überhaupt unter Geltungsbereich von Menschenrechtsinstrumenten fällt – beziehungs-

50 Heather Harrison Dinniss, Cyber Warfare and the Laws of War, Cambridge 2012, S. 2.

51 Bruce Schneier, Click Here to Kill Everybody, New York 2018, S. 3.

52 Schneier, supra, Fn. 51, S. 2–4.

53 Die Problematik ist am besten untersucht für die USA, s. z.B. Jennifer Stisa Granick, American Spies, Cambridge 2017.

weise ob die Regelung dieses Geltungsbereichs in Bezug auf den Cyberspace noch relevant ist.

5. Jurisdiktion und internationale Menschenrechtsverträge

Bei der Abgrenzung des Geltungsbereichs von völkerrechtlichen Menschenrechtsverträgen steht, wie eingangs erwähnt, die «Jurisdiktion» im Zentrum. Unglücklicherweise ist der Begriff der Jurisdiktion keineswegs eindeutig.[54] Im ursprünglichen Sinn ist Jurisdiktion die Kompetenz zum autonomen Erlass und zur autonomen Durchsetzung von Vorschriften, also in etwa die staatliche «Handlungsfähigkeit», die traditionell unterschieden wird in legislative, exekutive und judizielle Jurisdiktion.[55] Dieses Jurisdiktionsverständnis ist eng verknüpft (wenn auch nicht deckungsgleich)[56] mit dem Souveränitätsgedanken; sie ist sozusagen ein Ausfluss der Souveränität, wie der Ständige Internationale Gerichtshof schon im *Lotus*-Fall festhielt.[57] Da es hier um positive Rechte und Handlungsmöglichkeiten der Staaten geht, legen diese ihre Kompetenzen tendenziell weit und auch extra-territorial aus.[58] Jurisdiktion oder Hoheitsgewalt in diesem Sinne üben Staaten auch im Cyberspace aus. Sie erlassen Normen[59] und versuchen entsprechend, diese durchzusetzen.[60]

54 Insofern mag die österreichische Fassung der EMRK (supra, Fn. 12) zwar der den authentischen englischen und französischen Fassungen besser entsprechen als die Formulierung «Herrschaftsgewalt» (Jochen A. Frowein, «Probleme des allgemeinen Völkerrechts vor der Europäischen Kommission für Menschenrechte», in Ingo Münch & Hans-Jürgen Schlochauer (Hg.), Staatsrecht – Völkerrecht – Europarecht, Berlin 1981, S. 289, Fn. 1), bietet aber keinen Erkenntnisgewinn.

55 Vgl. Bernard H. Oxman, «Jurisdiction of States», Max Planck Encyclopaedia of International Law (2007), <http://opil.ouplaw.com/home/EPIL>, Para. 1.

56 Milanovič, supra, Fn. 8.

57 *Lotus,* PCIJ, ser. A no. 10 (1927), S. 19: *«[A State's] title to exercise jurisdiction rests in its sovereignty.»* – Der *Lotus*-Fall wird teilweise hochstilisiert zum Inbegriff eines souveränitätsbessessenen Völkerrechtsverständnisses, um sich dann umso besser von diesem überholten Verständnis abgrenzen zu können. Dabei wird oft übersehen, dass dieser Fall wegen Stimmengleichheit durch die Stimme des Präsidenten Max Huber entschieden werden musste (S. 32) und daher kaum als *Credo* des damaligen Völkerrechts taugt.

58 Klassisch etwa für die US-amerikanische Position U.*S. v. Aluminium Co. of America* (Court of Appeals for the Second Circuit), 148 F.2d 416 (2d Cir. 1945) (1945), S. 229. S. auch American Law Institute, Restatement of the Foreign Relations Law of the United States (Third), St. Paul, Minn. 1987, vol. 1, § 402 (Comment lit. d).

59 Ein aktuelles Beispiel ist Regulierung von Online-Glückspielen: Bundesgesetz vom 29. September 2017 über Geldspiele, SR 935.51 (angenommen in der Volksabstimmung vom 10. Juni 2018, BBl 2018 7755). In Österreich sind ähnliche Bestrebungen im Gang: Melany Buchberger-Golabi, «Internetblockaden gegen illegales Glücksspiel», Standard, 3. April 2018, S. 12.

60 *E.g.* Sentenza n. 4741/2000, Corte di Cassazione – Sezione V Penale (2000) (Online-Diffamierung); *La Ligue contre le racisme et l'antisémitisme c. Yahoo! Inc.* (Tribunal de grande instance), RG:00/0538 (2000) (Online-Verkauf von Nazi-Paraphernalia). Diesen Versuchen setzen konkurrierende Jurisdiktionsansprüche anderer Staaten jedoch Grenzen: *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme,* 433 F.3d 1199 (9th Cir.) (2006).

Dieses Konzept von Jurisdiktion ist jedoch nicht mit dem Jurisdiktionsbegriff identisch, wie wir ihn in der EMRK, im Uno-Pakt II und in anderen Menschenrechtsinstrumenten finden.[61] Hier geht es um den Anwendungsbereich des jeweiligen Instruments, also um den persönlichen oder räumlichen Umfang der vertragsstaatlichen Verpflichtungen. Und da es sich hiermit um staatliche Pflichten und nicht Rechte handelt, plädieren Staaten wenig überraschend für eine *enge* Auslegung.[62]

Eine dritte Bedeutung von Jurisdiktion schliesslich umschreibt die Kompetenz eines Gerichts. Hier handelt es sich um blosse Zulassungs- bzw. Zugangserfordernisse, welche die Zuständigkeit des Gerichts *ratione personae, materiae & temporis* umschreiben. Im Gegensatz zu diesen präliminären Kriterien bezieht sich die Frage der Hoheitsgewalt auf die substantielle Problematik, ob ein Staat durch den jeweiligen Vertrag gebunden ist.

Diese Frage stellt sich für alle Menschenrechtsinstrumente in ähnlicher Weise, doch ist die Rechtsprechung des EGMR zur «räumliche» Geltung der Konvention am weitesten entwickelt. Wie eingangs erwähnt, führt die historische Auslegung von Art. 1 EMRK zu einer territorial verstandenen Jurisdiktion. Der Gerichtshof, bzw. zuerst die Kommission, deuteten aber wiederholt gewisse Ausnahmen vom Territorialitätsprinzip an, etwa bei Inhaftierungen ausserhalb des Staatsgebiets oder in Bezug auf Handlungen von diplomatischem Personal im Ausland. In der Sache wurden diese Beschwerden aber abgelehnt.[63] Eine grundlegend weiteres Verständnis hatte jedoch bereits der Entscheid im Verfahren Zypern gegen die Türkei im Jahr 1975 etabliert. Im Zusammenhang mit der Besetzung Nordzyperns betonte die Kommission, dass Personen und Eigentum auch unter die Jurisdiktion eines Drittstaates gebracht werden können, sofern dieser Herrschaftsgewalt ausübt.[64] In allgemeinerer Weise wiederholte die Kommission diesen Grundsatz 1989 in *Drozd und Janousek*: Staaten tragen auch Verantwortung für hoheitliches Handeln, dass *Wirkung* ausserhalb des eigenen Territoriums zeitigt.[65] 1995 spezifizierte der Gerichtshof

61 *E.g.* Art. 3 International Convention on the Elimination of All Forms of Racial Discrimination, 21. Dezember 1965, 660 U.N.T.S. 212; Art. 2 Convention on the Rights of the Child, 20. November 1989, 1577 U.N.T.S. 44.

62 *E.g. Al-Skeini and Others v. United Kingdom,* supra, Fn. 18, Para. 109–119 (the Government's submission).

63 *Hess v. United Kingdom,* Application no. 6231/73, ECommHR, 28. Mai 1975; *X. v. Germany,* Application no. 92/35/81, ECommHR, 16. Juli 1982.

64 *Cyprus v. Turkey,* Application nos. 6780/74 and 6950/75 (Admissibility), ECommHR, 26. Mai 1975, S. 136, Para. 8: *«[A]uthorised agents of a State ... not only remain under its jurisdiction when abroad but bring any other persons or property »within the jurisdiction« of that State, to the extent that they exercise authority over such persons or property. Insofar as, by their acts or omissions, they affect such persons or property, the responsibility of the State is engaged.»*

65 *Drozd & Janousek v. France & Spain (Admissibility),* Application no. 12747/87, ECtHR, 12. Dezember 1989, Para. 91: *«The term <jurisdiction> is not limited to the national territory of the High Contracting Parties; their responsibility can be involved because of acts of their authorities producing effects outside their own territory.»*

dann (wieder im Zusammenhang mit dem Zypernkonflikt) einschränkend, dass in solchen Fällen immerhin eine «wirksame Gesamtkontrolle» *(«effective overall control»)* vorausgesetzt werde.[66]

In vergangenen Jahren verschärfte eine Reihe militärischer Aktionen von Europaratsmitgliedern die Problematik der Extra-Territorialität: die Interventionen von Nato-Mitgliedern im ehemaligen Jugoslawien, von Russland in Moldawien und vom Vereinigten Königreich in Afghanistan und Irak.[67] Der Gerichtshof reagierte auf diese Entwicklung zuerst sehr zurückhaltend: In *Banković* berücksichtigte er fast ausschliesslich das territoriale Element.[68] Diese Rechtsprechung wurde teilweise heftig kritisiert,[69] und der Gerichtshof revidierte sie in der Folge sukzessive. So hielt er in Zusammenhang mit Transnistrien fest, dass bereits ein «entscheidender Einfluss» auf ein Territorium die Geltung der Konvention aktiviere.[70] In zwei gegen Grossbritannien gerichteten Fällen verlangte der Gerichtshof dann nur *«authority and control»* des Mitgliedsstaates über die Beschwerdeführer, wobei auch temporäre Kontrolle ausreichen mag.[71]

Somit steht in der aktuellen Praxis zu Art. 1 EMRK das territoriale Element, also das eigene Staatsgebiet eines Mitgliedsstaates, zwar weiterhin im Vordergrund, wie der Gerichtshof bei jeder Gelegenheit wiederholt.[72] In *persönlicher* Hinsicht kann sich die Jurisdiktion über dieses Territorium hinaus ausdehnen, wenn Staatsakteure im Ausland unmittelbare physische Gewalt und Kontrolle ausüben – etwa bei Ent-

66 *Loizidou v. Turkey (Preliminary Objections),* Application no. 15318/89, ECtHR (Chamber), 23. März 1995, Para. 62.

67 *Banković and others v. Belgium and Others,* Application no. 52207/99, ECtHR (Grand Chamber), 12. Dezember 2001; *Ilaşcu and others v. Moldova and Russia,* Application no. 48787/99, ECtHR (Grand Chamber), 8. Juli 2004; *Al-Skeini and Others v. United Kingdom,* supra, Fn. 18; *Al-Jedda v. United Kingdom,* supra, Fn. 18. – Extra-Territorialität wurde auch thematisiert in *Behrami and Behrami v. France and Ruzhdi Saramati v. Germany and Norway (Admissibility Decision),* Application nos. 71412/01 & 78166/01, ECtHR (Grand Chamber), 2. Mai 2007, doch stand dort die Zuständigkeit *ratione personae* und das Verhältnis der EMRK zu Kapitel VII der UNO-Charta im Vordergrund (Para. 68–70).

68 *Banković and others v. Belgium and others,* supra, Fn. 67, Para. 59–61.

69 *E.g.* Rick Lawson, «Life After Banković», in: F. Coomans & M. T. Kamminga (Hg.), Extraterritorial Application of Human Rights Treaties, Antwerp 2004, 83–123; Loukis G. Loucaides, «Determining the Extra-Territorial Effect of the European Convention: Facts, Jurisprudence and the Bankovic Case», 11 European Human Rights Law Review (2006), 391–407; Marko Milanović, «From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties», 8 Human Rights Law Review (2008), 411–448.

70 *Ilaşcu and others v. Moldova and Russia,* supra, Fn. 67, Para. 392: *[The «Moldavian Republic of Transdniestria»] remains under the effective authority, or at the very least under the decisive influence, of the Russian Federation, … .*

71 *Al-Skeini and Others v. United Kingdom,* supra, Fn. 18, Para. 149; *Al-Jedda v. United Kingdom,* supra, Fn. 18, Para. 85.

72 *E.g. N.D. & N.T. v. Spain,* supra, Fn. 20, Para. 51.

führungen im Ausland,[73] oder mittels Kontrolle über ein Gebäude[74] oder eines Checkpoints innerhalb einer Sicherheitszone.[75] In *räumlicher* Hinsicht gilt die Konvention, wenn eines ihrer Mitglieder über fremdes Staatsgebiet effektive Kontrolle ausübt, ob mit oder ohne Zustimmung des betroffenen Staats.[76]

6. Menschenrechte, Jurisdiktion und Cyberspace

Was folgt nun aus dieser Praxis für den Falle eines Jeep Cherokee, dessen Bremsen elektronisch deaktiviert werden? Oder genauer: Inwieweit würde ein Staat, dessen Akteure den Bordcomputer kompromittieren, gegen menschenrechtliche Vertragspflichten verstossen, wenn die Manipulation etwa zum Tode der Insassen führt?[77] Auf die – äusserst komplexe – Frage der tatsächlichen Beweisführung gehe ich hier nicht ein.[78] Auch unterscheide ich nicht zwischen Staatsorganen und staatsnahen Akteuren. Es geht also ausschliesslich um die Frage, ob Staaten durch solches Handeln, durch Menschenrechtsverletzungen *im* oder *mittels* Cyberspace, ihre Verpflichtungen unter einzelnen Menschenrechtsverträgen verletzen.

Die Antwort zumindest des Tallinn-Manuals darauf ist eindeutig: *«International human rights law is applicable to cyber-related activities»*.[79] Das Manual nimmt dabei zwar auf Völkergewohnheitsrecht Bezug, doch kann die Aussage angesichts der identischen Thematik wohl ohne weiteres auch auf vertragliche Verpflichtungen übertragen werden (es ist kaum anzunehmen, dass gewohnheitsrechtliche Menschenrechtsnormen einen umfassenderen Geltungsanspruch enthalten als einschlägige Verträge, zumal diese oft eine salvatorische Klausel beinhalten)[80].

Die Experten des Manuals stützen sich auf die traditionellen Kriterien *(«power or effective control»),* jeweils in der Spielart des räumlichen oder persönlichen Mo-

73 *Öcalan v. Turkey,* Application no. 46221/99, ECtHR (Grand Chamber), 12 May 2005, Para. 91.

74 *Al-Jedda v. United Kingdom,* supra, Fn. 18, Para. 85.

75 *Al-Skeini and Others v. United Kingdom,* supra, Fn. 18, Para. 147.

76 *Ilaşcu and others v. Moldova and Russia,* supra, Fn. 67, Para. 315–316. – Für eine kritische und konzise Analyse der EGMR-Praxis s. auch Tilmann Altwicker, «Transnationalising Rights: International Human Rights Law in Cross-Border Contexts», 29 European Journal of International Law (2018), 588–590.

77 Es geht hier also nicht um die generelle völkerrechtliche Verantwortlichkeit oder *State responsibility;* diese ist zwar häufig kongruent mit Jurisdiktion i.S.v. Art. EMRK, aber nicht identisch.

78 Ein aktuelles Beispiel ist der Prozess *Mondelez Internationl Inc. v. Zurich American Insurance Company,* 2018 WL 4941760 (Ill. Cir. Ct.); die Versicherung schreibt die gegen die Ukraine gerichtete Cyberattacke *NotPetya* von 2017 dem russischen Staat zu und beruft sich deshalb auf den Deckungsausschluss bei einer *«hostile or warlike action»* (Jordan M. Rand, «My Least Favorite Exclusion Challenged by Milk's Favorite Cookie», Cyberinsurance Law Blog, 2. Januar 2019, <https://www.databreachninja.com/my-least-favorite-exclusion-challenged-by-milks-favorite-cookie/>).

79 Schmitt (ed.), supra, Fn. 38, Rule 34 (Applicability).

80 Vgl. Art. 5 Abs. 2 International Covenant on Civil and Political Rights [ICCPR], 16. Dezember 1966, 999 U.N.T.S. 172.; Art. 53 EMRK.

dells. Gerade in Bezug auf den hier zentralen Punkt konnten sie sich jedoch nicht einigen: ob eine solche Kontrolle auch *ohne* physisches Element ausgeübt werden könne. Eine Minderheit vertrat die Auffassung, dass ein Staat bereits effektive Kontrolle besitze, wenn er faktisch die Ausübung eines Individualrechts ausserhalb des eigenen Territoriums verhindern könne.[81] Die Mehrheit verneinte dies und hielt so an der traditionellen physischen oder kinetischen Dimension fest.[82]

Diese Dimension wird aber der ephemeren und proteischen Natur des Cyberspace kaum gerecht. Denn selbst bei dem «gekaperten» Jeep Cherokee kann man schwerlich von *physischer* Kontrolle ausgehen, da der Zugriff ja rein elektronisch, also in Form eines binären Computercodes erfolgt. Als Folge können Staaten Menschenrechtsverletzungen im Cyberspace nach der aktuellen *lex lata* weitgehend ungestraft begehen, solange dadurch Opfer ausserhalb ihres Territoriums betroffen sind. Diese Lücke muss geschlossen werden. Es gab zwar bisher kaum – zumindest in der Öffentlichkeit bekannte – Cyberattacken, die offensichtlich Individualrechte gefährdeten.[83] Aber es ist augenscheinlich, welches «Potential» hier ohne allzu lebhafte Vorstellungskraft aktiviert werden könnte. Einige Staaten scheinen bei extraterritorialen Aktionen inzwischen jegliche Hemmung verloren zu haben, und es ist nicht auszuschliessen – ja vielmehr absehbar –, dass sie dafür auch die virtuelle Welt nutzen werden.

Deshalb wäre ein neues und umfassenderes Jurisdiktionsverständnis geboten, das im Falle der EMRK auch die Rechte von Menschen ausserhalb des Konventionsraums besser berücksichtigt. Der EGMR könnte dafür sowohl auf Ansätze zurückgreifen, die einzelne Mitglieder in *separate opinions* äusserten,[84] wie auch auf die eigene Rechtsprechung, in der ein weites Jurisdiktionsverständnis bereits früh angelegt

81 So würde etwa die Meinungsäusserungsfreiheit eines Individuums verletzt, wenn ein Staat sich Zutritt zu dessen E-Mail-Konto verschafft und das Passwort ändert: Schmitt (ed.), supra, Fn. 38, Rule 34, Commentary, Para. 10.

82 Schmitt (ed.), supra, Fn. 38, Para. 6, 8, 9.

83 So etwa der WannaCry-Angriff, der den britischen *National Health Service* kompromittierte und damit das physische Wohl der Patienten wie auch deren Daten gefährdete (s. Committee on Public Accounts, Cyber-attack on the NHS, HC 787, House of Commons 18. April 2018). Die Überwachungsaktivitäten zahlreicher Geheimdienste wiederum verletzen das Recht auf Privatsphäre kontinuierlich (auch wenn sich hier ein gewisser Gewöhnungseffekt einzustellen scheint, s. supra, Fn. 47): *Big Brother Watch and Others v. United Kingdom,* Applications nos. 58170/13, 62322/14 & 24960/15, ECtHR (Chamber), 13. September 2018 (am 4. Februar 2019 an die Grosse Kammer verwiesen).

84 So etwa *Assanidze v. Georgia,* Application no. 71503/01, ECtHR (Grand Chamber), 8. April 2004, concurring opinion of Judge Loucaides: «*To my mind <jurisdiction> means* actual authority, *that is to say the* possibility of imposing the will of the State on any person, *whether exercised within the territory of the High Contracting Party or outside that territory. Therefore, a High Contracting Party is accountable under the Convention to everyone* directly affected by any exercise of authority by such Party in any part of the world. *Such authority may take different forms and may be legal or illegal. … the Convention provides a code of behaviour for all High Contracting Parties* whenever they act in exercise of their State authority with consequences for individuals.» (Hervorhebung durch den Autor).

ist. Schon 1975, anlässlich der Staatenbeschwerde Zyperns gegen die Türkei, stellte die Kommission auf die *Auswirkung* staatlicher Aktionen (oder Unterlassungen) auf Personen und Eigentum ab.[85] 1983 stellte wiederum die Kommission im Kontext der *Troubles* in Nordirland auf das Kriterium «aktiver Massnahmen» ab;[86] 1992 schliesslich fragte der Gerichtshof ebenfalls nach behördlichen Handlungen, die Wirkung ausserhalb des staatlichen Territorium zeitigten.[87]

In *Banković* lehnte dann die Grosse Kammer eine solche Auslegung zwar sinngemäss (und unter ungenauer Rekapitulation der früheren Rechtsprechung) mit dem Argument ab, dann könne ja jedermann weltweit Beschwerde erheben, sofern er durch die Handlung eines Mitgliedsstaats beeinträchtigt wurde.[88] Aber die Formulierung von Art. 1 EMRK erlaubt hier durchaus eine Differenzierung zwischen Abwehrrechten und Gewährleistungspflichten, zwischen *negative obligations* und *positive obligations*.[89] Auch hinsichtlich der Gewährleistungspflichten stellen sich im Cyberspace neue Herausforderungen und Probleme: Generell ist es für einen Staat schwierig und oft auch unmöglich, Grundrechte im Ausland zu gewährleisten. Es sollte aber kein Problem sein, auf menschenrechtswidrige Aktionen im Ausland zu *verzichten*. Dies ist auch kongruent mit der Minderheitsmeinung innerhalb der Tallinn-Expertengruppe, bei der ebenfalls die Auswirkungen staatlicher *Aktionen* entscheidend sein sollen.[90] Ein solcher Zugang liesse sich schliesslich auch unter dem Uno-Pakt für bürgerliche und politische Rechte – und damit auf universeller Ebene – begründen. Der Menschenrechtsausschuss hat in seiner Rechtsprechung keine expliziten Hürden für die extra-territoriale Anwendbarkeit des Paktes errichtet.[91] Und der Internationale Gerichtshof vertrat im Mauergutachten diese weite Auslegung ebenfalls – nicht nur für den Uno-Pakt II, sondern auch für den Uno-Pakt I und die Kinderrechtskonvention.[92]

85 *Cyprus v. Turkey,* supra, Fn. 64, S. 136, Para. 8 (wobei Jurisdiktion und Verantwortlichkeit nicht klar unterschieden werden).

86 *X. v. United Kingdom,* Application no. 9348/81, ECommHR, 28. Februar 1983, S. 199, Para. 5 *(«active measures»).*

87 *Drozd & Janousek v. France and Spain,* Application no. 12747/87, ECtHR (Plenary), 26. Juni 1992, Para. 91 *(«acts of their authorities producing effects outside their own territory»).*

88 *Banković and others v. Belgium and others,* supra, Fn. 67, Para. 75. Zur undeklarierten Modifikation der Rechtsprechung in Para. 71 (mit dem zusätzlichen Kriterium der *public powers*) s. Lawson, supra, Fn. 69, S. 111.

89 Zur Gewährleistung ausführlich Michael Holoubek, Grundrechtliche Gewährleistungspflichten, Wien 1997, und Alastair R. Mowbray, The Development of Positive Obligations Under the European Convention on Human Rights by the European Court of Human Rights Oxford 2004.

90 Schmitt (ed.), supra, Fn. 38, Para. 10: *«A few of the Experts took the position that … if an individual cannot exercise a human right or enjoy the protection of one because of a State's action, international human rights law applies extraterritorially».*

91 *López Burgos v Uruguay,* Communication no. 52/1979, CCPR, 29. Juli 1981, Para. 12.3.

92 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion,* 9. Juli 2004, I.C.J. Reports 2004, S. 136, Para. 111.

Besonders anschaulich für ein solches zeitgemässes Verständnis menschenrechtlicher Verpflichtungen ist die *Maison de l'escargot*-Analogie, die Luigi Condorelli im Kontext militärischer Interventionen propagiert hat.[93] Danach gleicht die Beziehung zwischen Staat und Jurisdiktion der Beziehung einer Schnecke zu ihrem Haus: Wo immer die Schnecke hingeht, folgt das Haus – und wo immer der Staat als Staat tätig wird, trägt er seine menschenrechtlichen Verpflichtungen mit sich.[94]

7. Fazit

Der Grundsatz *«don't panic»* gilt nicht nur für Reisen per Anhalter durch die Galaxie, sondern auch für die (rechtliche) Navigation im Cyberspace. Es ist wenig konstruktiv, wenn wir uns auf phantasievolle Vorstellungen über möglichst ausgeklügelte Cyberattacken kaprizieren.[95] Die Gefahr aber, dass der idealistische Traum der ersten Kybernauten vom herrschaftsfreien Bereich zum Albtraum einer (menschen-)rechtslosen Zone wird, ist real. Die Regierungen (nicht nur der Industriestaaten), diese angeblich «müden Giganten aus Fleisch und Stahl», haben inzwischen durchaus effektive und furchteinflössende Mittel und Wege der Machtausübung im digitalen Raum gefunden.[96] Die Welt des Cyberspace mag zugleich überall und nirgendwo sein und seine Avatare nicht physisch präsent.[97] Aber diese Avatare haben die eigene Körperlichkeit keineswegs transzendiert. Sie bleiben verletzlich in der physischen Welt. Und auch wenn sie über die ganze Erde verteilt sind – ihre Gedanken sind nicht vor Überwachung geschützt, ja sie haben inzwischen jeden Grund, sich vor unfreiwilliger Konformität oder erzwungenem Schweigen zu fürchten.[98]

Die Menschenrechte bleiben also auch in der digitalen Sphäre fragil; möglicherweise sind sie sogar noch exponierter als in der physischen Welt. Dort schränken räumliche Distanzen den hoheitlichen Zugriff auch ein: Über das eigene Territorium hinaus waren bisher die Handlungsmöglichkeiten staatlicher Akteure gering bzw. mit ganz erheblichem (militärischem) Aufwand verbunden. Es gab deshalb auch lange nur vereinzelt Anlass, die menschenrechtlichen Verpflichtungen von Staaten

93 Luigi Condorelli, «La protection des droits de l'Homme lors d'actions militaires menées à l'étranger», 32 Collegium (2005), S. 95; Luigi Condorelli, «Some Thoughts about the Optimistic Pessimism of a Good International Lawyer», 21 European Journal of International Law (2010), 33.

94 Condorelli, Protection, supra Fn. 93, S. 95: *«[L'Etat] transporte avec lui ses obligations en matière de droits de l'homme, tel – pourrait-on dire – un escargot qui ne saurait se promener autrement qu'avec sa propre maison sur le dos.»*

95 Wie dies etwa der Titel «Click Here to Kill Everybody» von Bruce Schneiers Buch nahelegt, supra Fn. 51 (ironischerweise impliziert die Titelillustration zugleich, dass dieser «Klick» nur zu einer Reihe von Fehlermeldungen führt: <https://www.schneier.com/books/click_here/>).

96 Vgl. Barlow, supra, Fn. 1 & Fn. 28.

97 Vgl. Barlow, supra, Fn. 30 & Fn. 31.

98 Vgl. Barlow, supra, Fn. 31, al. 8, und Fn. 32.

jenseits des eigenen Hoheitsgebiets zu thematisieren. Der Cyberspace aber schafft als schwer fass- und definierbarer (Nicht-)Raum neue, noch schwer quantifizierbare Potentiale für die Verletzung von Menschenrechten.

Als Folge müssen wir auch das tradierte, immer noch überwiegend territorial konstruierte Konzept des Anwendungsbereichs von Menschenrechtsinstrumenten hinterfragen. Zwar wurde das herkömmliche Jurisdiktionsverständnis insbesondere als Folge der «humanitären Interventionen» vor und nach der Jahrtausendwende selektiv sowohl persönlich wie auch räumlich erweitert. Aber diese nach wie vor als Ausnahmen verstandenen Ergänzungen werden den kategorial neuen faktischen und rechtlichen Herausforderungen des Cyberspace nicht gerecht.

Entsprechend dringend wäre ein extensiver Zugang, eine grosszügigere Auslegung der staatlichen Hoheitsgewalt. In Bezug auf Menschenrechtsverletzungen im oder mittels Cyberspace ist ein konsequentialistisches Jurisdiktionsverständnis erforderlich, das sich primär an den individualrechtlich relevanten Folgen (para-)staatlichen Handelns ausrichtet. Dafür gibt es auch erste Ansätze in der Praxis.[99] Denn zumindest in menschenrechtlicher Hinsicht muss für die Staaten gelten: *Cyberspace does lie within your borders.*

99 *E.g.* supra Fn. 84, *in fine.*